



# CVE-2020-8649

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2020-8649
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-02-06 01:15:00 UTC
<b>Updated</b>	2021-12-30 20:44:00 UTC
<b>Description</b>	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the vgacon_invert_region function in drivers/video/

## Risk And Classification

**Problem Types:** CWE-416

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Linux</a>	<a href="#">Linux Kernel</a>	All	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All

## References

Reference	Source	Link	Tags
206357 – Linux Kernel 5.4.7 - vgacon_invert_region use-after-free	MISC	<a href="#">bugzilla.kernel.org</a>	Exploit, Issue Tracking, Vendor
[SECURITY] [DLA 2241-2] linux security update	MLIST	<a href="#">lists.debian.org</a>	
[security-announce] openSUSE-SU-2020:0388-1: important: Security update	SUSE	<a href="#">lists.opensuse.org</a>	Third Party Advisory
[SECURITY] [DLA 2242-1] linux-4.9 security update	MLIST	<a href="#">lists.debian.org</a>	
[SECURITY] [DLA 2241-1] linux security update	MLIST	<a href="#">lists.debian.org</a>	
Debian -- Security Information -- DSA-4698-1 linux	DEBIAN	<a href="#">www.debian.org</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[159684](#) Oracle Enterprise Linux Security Update for kernel (ELSA-2020-4431)

[240197](#) Red Hat Update for kernel-rt (RHSA-2022:1209)

[240198](#) Red Hat Update for kernel (RHSA-2022:1213)

[377065](#) Alibaba Cloud Linux Security Update for cloud-kernel (ALINUX2-SA-2020:0113)

[750691](#) SUSE Enterprise Linux Security Update for the Linux Kernel (SUSE-SU-2020:1141-1)

[900078](#) CBL-Mariner Linux Security Update for kernel 5.4.91

[903383](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1933)

[905836](#) Common Base Linux Mariner (CBL-Mariner) Security Update for kernel (1933-1)

[940256](#) AlmaLinux Security Update for kernel (ALSA-2020:4431)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**